HIPAA Template Draft

Title	**INFORMATION SECURITY: RISK ANALYSIS AND MANAGEMENT**	
Creation		
Date	02/22/01	
Author	Dana Kleiman/ Maria Dedet	Mina Martel
Phone number	916/ 654-9381	916/ 654-2214
Email address	dkleiman@edd.ca.gov	mmartel@dds.ca.gov
Revision		
Date		
Author		
Phone number		
Email address		

Introduction

This is a template on developing Risk Analysis and Risk Management measures for the protection of data and information assets affected by HIPAA rules and regulations.

Purpose

HIPAA's Final Rule, Part 164 (Security and Privacy) mandates the protection of the confidentiality of individual medical data/records. This document acts as a guide for compliance with HIPAA requirements for the risk analysis and risk management of these information assets.

Assumptions, Pre-requisites, and Dependencies

"Each state department or state agency shall designate a position within the department or agency, the duties of which shall include, but not be limited to, responsibility for the privacy policy within that department or agency." –SB No. 129, Chapter 984: a position must be designated.

Responsibility for review and monitoring of plans will be under a department/ agency level Security Officer and/or Privacy Officer.

The Security Officer and/or Privacy Officer will have responsibility to coordinate with IT system administrators to establish authorities for access to confidential data. Levels of access must be established for both employees and other authorized users of the information assets of the department or agency.

Policies and procedures to protect data will be designed and in place for each state department or agency. If State law is more stringent than Federal, State law will be followed.

Confidentiality Statement and/or Access Control Statement to be signed by the authorized user and/or owner of the data will be in place and part of regular security practices.

A system will be in place to report violations or incidents.

Sanctions for non-compliance will be part of the policies and procedures.

Training will occur at work unit level and at regular intervals to maintain employee security awareness.

All applicable laws, rules, regulations unique to each state agency will be included in development of their templates, business practices, policies and guidelines.

Constraints

Time
Any deadline on meeting compliance requirements
Time available for review of work-unit plans or form submissions
Timing of reviews…how often, what time of year, etc.

Personnel
Are there agency Security Officers? Who else has authority?
Are there sufficient personnel to review work-unit plans/forms? Are they available?
Are their skill sets sufficient?

Resources
Materials
Facilities
Access
Authorities
Funding/ Budget
Personnel

Authorities
Security Officer
Privacy Officer
IT unit
Information Security Unit
Who has ultimate responsibility for program? To determine business need for authorities?
Who (or what position) will be the agency contact?
What controls are in place for actions of Covered Entities (Health Plans, Clearinghouses, Health Providers), Hybrid Entities, Affiliated Covered Entities and Business Associates (including Subcontractors and Agents)?
What are the legislative, regulatory or policy-related mandates specific to the operations and business practices of each agency or department?

Process

Identify and Evaluate

Each agency or department shall determine if it is affected by the HIPAA Rule. (see PSN's free internet HIPAA Calculator Report: http://www.privacysecuritynetwork.com/healthcare/hipaa/default. cfm. Also, refer to the Covered Entity template).

Each agency or department affected by the HIPAA Rule must:

identify the data or information asset to be protected, including systems, personnel and equipment.

determine the critical value/ risk level of the identified data or information asset (see SAM 4840.4: Definitions).

identify what may adversely affect the data or information asset.

determine acceptable risk levels based on probability of the event, probability of financial loss (including personnel hours) or legal action, and vulnerabilities of the organization.

Identify and Assign

Each agency or department affected by the HIPAA Rule shall:

identify and assign levels of risks in accordance with the information or data owned or maintained and the probability or severity of losses.

identify safeguards to reduce negative effects of data or information loss, modification, destruction or damage, misuse, or unauthorized access or disclosure and reduce the likelihood that such events will occur.

Plan

Each agency or department affected by the HIPAA Rule shall:

develop a plan for selecting and implementing cost-effective or critical safeguards.

develop policies, procedures, processes, standards and guidelines to support the protection and security of its data or information assets.

create, review or amend its existing Business Continuity Plan. Continuity Plans must include security measures for the protection of data or information assets affected by the HIPAA Rule.

Implement

Each agency or department affected by the HIPAA Rule shall:

develop and deliver security training to all employees, business partners and other data or information users, as appropriate.

institute and follow measures for the authorized destruction of data or information assets (e.g. tape swipes, paper shredders).

Procedures

Identify and Ev**aluate**

Each agency or department shall determine if the HIPAA Rule affects it (see PSN's free internet HIPAA Calculator Report: http://www.privacysecuritynetwork.com/healthcare/hipaa/default. cfm. Also, refer to the Covered Entity template).

If affected by the HIPAA Rule, the agency or department shall:

identify the data or information asset to be protected, including systems, personnel and equipment (see SAM, Section 4840-4845).

create a checklist which identifies risks and vulnerabilities involved in the release of information to a variety of users (see Attachment No. 1 – Risk Analysis Questionnaire).

assign a critical value/ risk level to the data or information asset based on the risks and vulnerabilities identified.

Procedures useful in the identification and evaluation of risk are:
Brainstorming
Physical, logical or theoretical walk-throughs of a process, system, life cycle or facility
Flowcharts of procedure or process flows, floor plans, network or system configurations, etc.
Review of historical information, including evaluations, audits, compliance reviews, issue memos, incident reports generated during the normal course of business.
Use of existing internal materials, externally published materials and internet sites which deal with the subjects of risk analysis and risk management.

Identify and Assign

Each agency or department shall create a list of possible consequences to support the determination of risk level (see Attachment No. 2 – Listing of Consequences).

Determination of risk level and consideration of acceptable risk should be based on:
Probability of a risk's occurrence
Percentage of likelihood
Ratio
Number of occurrences within a specified time period
Value
Loss Hours (increase in staff hours if event occurs)
Cost of Loss Hours
Consequences
Financial loss
Liability
Bad publicity
Loss of credibility or public trust
Loss of life or injury
Impact on workload, personnel or facilities
Impact on ability to meet federal and/or state legislative mandates

Each agency or department shall review its existing practices and identify where security of information assets (including but not limited to, systems, personnel and equipment,) may be improved.

An additional tool for Risk Management is DOIT's Risk Management Plan
(http: //www.doit.ca.gov/SIMM/Project Management/docs/sb5rmw.doc).

Plan

Each agency or department shall create, alter or amend existing security policies, procedures, guidelines and practices to include security considerations for the protection of HIPAA sensitive or confidential information (see Attachment No. 3 – Summary of British Standard 7799 – 1:1999).

Each agency or department shall research safeguards and methods to mitigate identified risks and vulnerabilities specific to HIPAA (e.g. Attachment No.. 4 – Data Handling Matrix). Some safeguards to be considered are:
computer programs and controls
authenticaton
access authorizations

firewalls
equipment and facility access controls
personnel practices
security in the workstations (direction of monitors, etc.)
security awareness training

A plan should be developed to implement those safeguards and mitigations which are most cost effective or which are critical.

Each agency or department shall develop a Business Continuity Plan to address security concerns in the event of a disaster which shall consist of both an Emergency Response Plan and a Business Resumption Plan.

Implement

Each agency or department shall institute practices to reduce security risks and shall review them periodically.

Each agency or department should perform a “dry run” of their Business Continuity Plan on an annual basis.

Infor**mation Concerns**

Confidentiality – secure information from unauthorized disclosure

Integrity – safeguard the accuracy and completeness of data and information

Availability – ensure information assets are available when required

Monitoring compliance cr**iteria**

Accountability
What are the levels of accountability?
Individual positions should be assigned for the following levels of responsibility:
Creation of the policies, standards, practices, procedures and guidelines which protect the security of HIPAA sensitive or confidential data or information assets
Implementation of those policies, standards, practices, procedures and guidelines
Maintenance of those policies, standards, practices, procedures and guidelines
Monitoring of compliance with those policies, standards, practices, procedures and guidelines
Enforcement of those policies, standards, practices, procedures and guidelines

Federal
HIPAA - go to website: **http://www.hhs.gov/ocr/hipaa/.**
Also refer to:
Federal Privacy Act
Federal Computer Fraud Act
Freedom of Information Act
Law 42 USC Section 503 of the Social Security Act

State

SB19 - go to website: **http://www.leginfo.ca.gov/pub/bill/sen/sb_19_bill_19990929_chaptered.html**
Also refer to:
Information Practices Act (Civil Code Section 1798)
Comprehensive Computer Data Access and Fraud Act (Penal Code Section 502)
Public Records Act (Government Code Section 6250)
the SAM
the California Unemployment Insurance Code (Section 2714) provides guidelines for Disability Insurance disclosure of medical information.

Glossary of terms

Go to website**:** **http://www.wedi.or/public/articles/hipaaglossary.pdf**

ATTACHMENT NO. 4 – DATA HANDLING MATRIX (SAMPLE)

NOTES	HANDLING CONCERN	HIPAA RESTRICTED
Mitigation of risk if faxing: Cover for fax must: Warn against misuse Require return to originator and notification if received by wrong party State legal requirements and itemize sanctions if violated Confirmation page from originator's fax machine must show: Transmission was successful Phone number receiving transmission Date and time must be kept current and printed or printable (i.e. log vs individual confirmations) If transmission log used, must be kept in a central location, and available Recipient should be notified of impending fax and be on hand when it comes through the machine on that end.		
	STORING	
	Storage on Fixed Media (e.g., Hard Drive)	Encryption and physical access controls
	Storage on Exchangeable Media (e.g., floppy disk)	Encryption and physical access controls
	MANIPULATING	
	Copying	Permission of data subject or individual who is the subject of the request
	Faxing	Not advised. Mitigations required (see below)
	Electronic Media Labeling Required	Internal and external labels required

	Hard Copy Labeling Required	Each page if not bound. If bound, front & back covers and title page
	Internal Mail	Indicate addressee only on interoffice envelope. Indicate addressee and “ Confidential - Personal Medical Information” AND “For eyes of ______ Only” on sealed internal envelope
	External Mail	Indicate addressee and “Restricted Delivery” on sealed envelope. Send by certified mail, restricted delivery
	RELEASING	
	Granting Access Rights	Data subject only or by court order to data owner
	Release to Third Parties	Only as permitted by law, authorized by data subject, or court order
	Sending by Public Network (e.g. Internet)	Not advised. If used, data must be encrypted at both sender and receiver ends and access must be at an authorized level.

ATTACHMENT NO. 2- LISTING OF CONSEQUENCES

Item	**Consequence**
No.	
1	Cost overrun of less than 10%.
2	Cost overrun of more than 10%.
3	Project takes up to 10% longer to complete than projected.
4	Project takes more than 10% longer to complete than projected.
5	Project fails to meet business objectives.
6	Some functional requirements get dropped.
7	Department fails to meet state/federal mandated timeframes for project implementation.
8	Non-compliance with federal and/or state regulations, laws, requirements, etc.
9	Unauthorized disclosure of confidential or sensitive information.
10	Malicious code attacks.
11	Unable to recover system within required timeframes.
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	

Attachment No. 1 - RISK ANALYSIS QUESTIONNAIRE

QUESTIONS	Degree Practice Is Followed	Not Applicable	Don't Know
1. Access to user workstation area is limited to authorized and validated users only?			
2. Are there visitor control procedures?			
3. Do office staff always challenge unescorted or improperly badge/identified visitors?			
4. The office has well-defined, current and useful operating procedures?			
5. The office has a quality assurance and performance monitoring programs?			
6. The office analyzes operational problems, such as those caused by rapid systems change, high turnover rate, lack of well-defined procedures, and under staffing?			
7. The office has effective and verifiable input and output control systems to ensure that authorized and validated data only is entered, and that printouts and other media are provided to authorized individuals only?			
8. The office verifies the identify of authorized personnel prior to releasing negotiable instruments such as cashable checks?			
9. A system exists to track the receipt, processing, and return of personnel documents submitted to Payroll Services Section for action?			
10. Workstation users always log-off the system when they leave their workstation area?			
11. The training provided to the operators and users is current and sufficient to minimize most data entry errors and to reduce the likelihood of data contamination and destruction?			
12. The office follows established confidentiality policy and procedures?			
13. The office has developed an effective on-going training system and procedures to ensure that personnel are informed of security and confidentiality requirements?			
14. All office employees have signed a data confidentiality statement?			
15. All employees are familiar with the information Security Office (ISO) and its role in the overall information and system security programs?			
16. All employees are aware of who the Information Security Specialist is in their office?			
17. All confidential documents are accounted for and secured?			
18. Printed output(i.e., letters, memos, charts, manuals) that contain confidential information are protected from improper disclosure and properly destroyed?			
19. In response to telephone inquiries, employees furnish non-confidential information freely but restrict confidential information to authorized inquirers only?			
20. Users are required to change the initial system passwords before allowed access to the system or network?			

21. Passwords are changed quarterly and when renewed, are not the same or significantly similar
to a previous password?

22. Employees use only their user ID and password, and never allow another individual to use
their user ID and password?

23. Employees never log onto a terminal for another person to use?

24. Users virus check all downloaded files, and keep virus protection programs current?

25. The office's network and systems are reliable and provide maximum availability, response,
and support to the users?

26. Network administrators and users are trained on the weaknesses of their network and how
easily these weaknesses may be exploited with internet access?

27. Data and other information are always properly stored when not in use?

28. Tape and disks are labeled externally (on the cover) with the creation date, description of
contents, data classification level, name of data owner, and unique control number?

29. Workstation users are restricted by operating systems, applications, and organization
policy from logging on to more than one workstation at a time?

30. Are employees and supervisors aware of fire alarm switch locations?

31. Applicable emergency evacuation instructions have been disseminated and clearly posted?

32. Posted emergency evacuation route charts indicate an assembly point so supervisors can
verify that all personnel are out of the building?

33. Documented procedures exist and training is provided to guide users in the recovery and
backup of data from servers or PC hard-disks?

34. Users are responsible for their own hard-disk backup?

35. In the event of an emergency or disaster, there is a formal written plan for Emergency
Response , easily available?

36. In the event of an emergency or disaster, there is a formal written plan for Business Resumption,
easily available?

37. Actions to protect equipment from disruption or damage have been taken? (e.g. tiedowns,
surge protectors, etc.).

38. Critical business functions have been identified?

39. Alternate sites for business resumption in case of emergency or disaster have been
identified and periodically are reviewed?

40. Method of emergency notification includes consideration for handicapped individuals?

Asset: Something of value, which is of use to an organization in accomplishing its goals. Assets may be tangible (physical) or intangible (information, political).

Vulnerability: A weakness or flaw in an organization's Electronic Data Processing (EDP) environment or other operations that, if left uncorrected, makes it susceptible to threats.

Threat: A natural or human event or act, such as an earthquake, fire, flood, error or fraud, that results in a loss to the organization.

Safeguard: A technique, procedure or device, such as a "firewall,' that is intended to minimize or eliminate the possibility of a threat successfully exploiting a vulnerability.

Risk: Asset X Vulnerability X Threat = Risk

Risk Analysis: The application of a standardized methodology in the determination of threats, risk factors, vulnerability exposures and potential losses. Risk Analysis is an approach to satisfying the need of an organization to protect the assets in which it has made an investment. It also serves to identify the particular problems an organization could expect to encounter in the performance of its mission, and the adverse affects these problems might present to the organization's ability to meet its obligations. Finally, risk analysis is a mechanism by which management can address these problems according to their relative importance bases on financial analysis, and develop safeguards which are both reasonable and cost-effective.

The process includes: identifying assets, determining their value, identifying what may adversely affect them, determining by what means and how often they may be affected; identifying safeguards to reduce the likelihood of negative effects; and determining a plan for selecting and implementing cost-effective safeguards.

DRAFT Attachment #4

ATTACHMENT NO. 3 – SUMMARY OF BRITISH STANDARD 7799 – 1:1999

Security Policy
Top management should set a clear direction and demonstrate their support for and commitment to information security through the issuance of an Information Security Policy effective across the organization. (3.1)

Security Organization
The objective of the information security infrastructure is to manage information security within the organization. A management framework should be established to initiate and control the implementation of information security within the organization. Responsibilities for the protection of individual assets and for carrying out specific security processes should be explicitly defined. (4.1 and 4.1.3)

Asset Classification and Control
The objective of assigning accountability for information assets is to maintain appropriate protection of organizational assets. All major information assets should be accounted for and have a nominated owner. Inventories should be maintained of all major information assets. (5.1)

Personnel Security
The objective of personnel security is to reduce the risks of human error, theft, fraud or misuse of facilities. Security should be addressed at the recruitment stage, included in job descriptions and contracts, and monitored during an individual's employment. (6.1)

Physical and Environmental Security
The objective of physical and environmental security is to prevent unauthorized access, damage and interference to IT services. IT facilities supporting critical or sensitive business activities should be physically protected from security threats and environmental hazards. (7.1)

Computer and Network Management
The objective of network and data center management controls is to ensure the correct and secure operation of computer and network facilities. Responsibilities and procedures for the management and operation of all computers and networks should be established. (8.1 and 8.5)
System Access Control

Access to computer services and data should be controlled on the basis of business services including computer systems, network services, applications and data. To detect unauthorized users or activities, systems should be monitored. (9.1, 9.2 and 9.7)

Systems Development and Maintenance
Security requirements should be identified and agreed prior to the development of IT systems to ensure that security is built into IT systems. (10.1)

Business Continuity Planning
Business continuity plans should be available to protect critical business processes from the effects of major failures or disasters. (11.1)

Compliance

The objective of security monitoring is to ensure compliance with organizational security policies and standards, and applicable laws. The security of IT systems should be regularly reviewed. (12.2)